

**WHAT IS CLAIMED IS:**

- 1 1. A method for securing data, said method comprising:  
2 receiving a first password corresponding to a software  
3 application;  
4 generating a first mask value based on the first  
5 password;  
6 combining the first mask value with a first encryption  
7 key, wherein the first encryption key is derived  
8 from a generated key and a known value, the  
9 combining resulting in a tied key;  
10 receiving a second password corresponding to the  
11 software application;  
12 generating a second mask value based on the second  
13 password;  
14 separating a recovered encryption key from the tied  
15 key using the second mask value, the recovered  
16 encryption key including a recovered generated  
17 key and a recovered known value; and  
18 encrypting data using the recovered generated key.
- 1 2. The method as described in claim 1 further comprising:  
2 encrypting the tied key using a second encryption key,  
3 the encrypting resulting in a first encrypted  
4 tied key; and  
5 returning the first encrypted tied key to the software  
6 application.
- 1 3. The method as described in claim 2 further comprising:  
2 receiving a second encrypted tied key; and  
3 combining the second encrypted tied key with the  
4 second encryption key, the combining resulting in  
5 a recovered tied key.

1 4. The method as described in claim 2 further comprising:  
2 determining whether a matched encryption tied key is  
3 available corresponding to the second encryption  
4 key; and  
5 sending the matched encryption tied key to a security  
6 module in response to the determination.

1 5. The method as described in claim 2 further comprising:  
2 determining whether a matched encrypted tied key is  
3 available corresponding to the second encryption  
4 key; and  
5 sending the first password to a security module in  
6 response to the determination.

1 6. The method as described in claim 1 further comprising:  
2 determining whether the recovered known value is  
3 correct; and  
4 processing a data file based on the determination.

1 7. The method as described in claim 6 wherein the  
2 processing is selected from the group consisting of  
3 encrypting the data file using the recovered generated  
4 key and decrypting the data file using the recovered  
5 generated key.

1 8. An information handling system comprising:  
2 one or more processors;  
3 a memory accessible by the processors;  
4 one or more nonvolatile storage devices accessible by  
5 the processors;  
6 a hardware security module accessible by the  
7 processors;

8 a data security tool for securing data using the  
9 hardware security module, the data security tool  
10 including:  
11 means for receiving a first password corresponding to  
12 a software application;  
13 means for generating a first mask value based on the  
14 first password using the hardware security  
15 module;  
16 means for combining the first mask value with a first  
17 encryption key using the hardware security  
18 module, wherein the first encryption key is  
19 derived from a generated key and a known value,  
20 the combining resulting in a tied key;  
21 means for receiving a second password corresponding to  
22 the software application;  
23 means for generating a second mask value based on the  
24 second password using the hardware security  
25 module;  
26 means for separating a recovered encryption key from  
27 the tied key using the second mask value, the  
28 recovered encryption key including a recovered  
29 generated key and a recovered known value; and  
30 means for encrypting data using the recovered  
31 generated key.

- 1 9. The information handling system as described in claim  
2 8 further comprising:  
3 means for encrypting the tied key using a second  
4 encryption key, the encrypting resulting in a  
5 first encrypted tied key; and  
6 means for returning the first encrypted tied key to  
7 the software application.

1 10. The information handling system as described in claim  
2 9 further comprising:  
3 means for receiving a second encrypted tied key; and  
4 means for combining the second encrypted tied key with  
5 the second encryption key using the hardware  
6 security module, the combining resulting in a  
7 recovered tied key.

1 11. The information handling system as described in claim  
2 9 further comprising:  
3 means for determining whether a matched encryption  
4 tied key is available corresponding to the second  
5 encryption key; and  
6 means for sending the matched encryption tied key to  
7 the hardware security module in response to the  
8 determination.

1 12. The information handling system as described in claim  
2 8 further comprising:  
3 means for determining whether the recovered known  
4 value is correct; and  
5 means for processing a data file corresponding to the  
6 determination.

1 13. The information handling system as described in claim  
2 12 wherein the means for processing is selected from  
3 the group consisting of a means for encrypting the  
4 data file using the recovered generated key and a  
5 means for decrypting the data file using the recovered  
6 generated key.

1 14. A computer program product stored in a computer  
2 operable media for securing data, said computer  
3 program product comprising:  
4 means for receiving a first password corresponding to  
5 a software application;  
6 means for generating a first mask value based on the  
7 first password;  
8 means for combining the first mask value with a first  
9 encryption key, wherein the first encryption key  
10 is derived from a generated key and a known  
11 value, the combining resulting in a tied key;  
12 means for receiving a second password corresponding to  
13 the software application;  
14 means for generating a second mask value based on the  
15 second password;  
16 means for separating a recovered encryption key from  
17 the tied key using the second mask value, the  
18 recovered encryption key including a recovered  
19 generated key and a recovered known value; and  
20 means for encrypting data using the recovered  
21 generated key.

1 15. The computer program product as described in claim 14  
2 further comprising:  
3 means for encrypting the tied key using a second  
4 encryption key, the encrypting resulting in a  
5 first encrypted tied key; and  
6 means for returning the first encrypted tied key to  
7 the software application.

1 16. The computer program product as described in claim 15  
2 further comprising:

3 means for receiving a second encrypted tied key; and  
4 means for combining the second encrypted tied key with  
5 the second encryption key, the combining  
6 resulting in a recovered tied key.

1 17. The computer program product as described in claim 15  
2 further comprising:  
3 means for determining whether a matched encryption  
4 tied key is available corresponding to the second  
5 encryption key; and  
6 means for sending the matched encryption tied key to a  
7 security module in response to the determination.

1 18. The computer program product as described in claim 15  
2 further comprising:  
3 means for determining whether a matched encrypted tied  
4 key is available corresponding to the second  
5 encryption key; and  
6 means for sending the first password to a security  
7 module in response to the determination.

1 19. The computer program product as described in claim 14  
2 further comprising:  
3 means for determining whether the recovered known  
4 value is correct; and  
5 means for processing a data file corresponding to the  
6 determination.

1 20. The computer program product as described in claim 19  
2 wherein the means for processing is selected from the  
3 group consisting of a means for encrypting the data  
4 file using the recovered generated key and a means for

```
5      decrypting the data file using the recovered generated
6      key.
```